```
Set     Items   Description
S1      91086   INTRUD? OR INTRUS? OR IDD OR IDDS OR IDS OR HONEY()POT? ? -
             OR SAND()BOX OR SANDBOX? OR NSM? OR THREAT()MONITOR? OR SURVE-
             IL? OR (ANOMAL? OR MISUSE?)(3N)(DETECT? OR MONITOR?)
S2     209568   KERNEL? OR CORE? OR CENTRAL()(PROGRAM? OR MODULE?) OR SYST-
             EM()(LEVEL? OR PROGRAM?)
S3     290106   BUFFER? OR CACHE? OR TEMPORAR?()(MEMOR? OR STORAGE?) OR CI-
             RCULAR()BUFFER?
S4      25191   DEVICE()DRIVER? OR DDL OR (PERIPHERAL? OR DEVICE)(N)(IO OR
             I()O OR INTERFACE?)
S5     478004   AUDIT? OR MONITOR? OR LOG OR LOGS OR LOGGING OR LOGGED OR -
             HISTOR?
S6        308   S1 (10N) S2
S7          1   S6 (10N) S3
S8          0   S6 (10N) S4
S9         35   S6 (10N) S5
S10        82   S1(S)S2(S)S3
S11        15   S6(10N)INTERFACE?
S12        40   S10(S)(S4 OR S5)
S13        80   S9 OR S12 OR S11
S14        22   S13 AND IC=(G06F-012? OR G06F-007? OR G06F-017? OR H04L-00-
             9?)
S15        22   IDPAT (sorted in duplicate/non-duplicate order)
S16        22   IDPAT (primary/non-duplicate records only)
File 348:EUROPEAN PATENTS 1978-2005/Feb W03
        (c) 2005 European Patent Office
File 349:PCT FULLTEXT 1979-2002/U
```

16/3,K/6 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00952584 **Image available**
SYSTEM AND METHOD FOR ANALYZING LOGFILES
SYSTEME ET PROCEDE D'ANALYSE DE FICHIERS DE TRACE
Patent Applicant/Assignee:
RECOURSE TECHNOLOGIES INC, 1600 Seaport Blvd., Suite 400, Redwood City,
CA 94063, US, US (Residence), US (Nationality)
Inventor(s):
SORKIN Stephen, 810 Coleman Ave. #16, Menlo Park, CA 94025, US,
LYLE Michael, 2844 Buena Knoll Court, San Jose, CA 95121, US,
ROSS Robert F, 151 Calderon #334, Mountain View, CA 94041, US,
MARICONDO James R, 872 Ames Court, Palo Alto, CA 94303, US,
Legal Representative:
YI Susan C (agent), Van Pelt & Yi, LLP, 4906 El Camino Real, Suite 205,
Los Altos, CA 94022, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200286724 A1 20021031 (WO 0286724)
Application: WO 2002US12936 20020423 (PCT/WO US0212936)
Priority Application: US 2001841689 20010423
Designated States:
(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL
TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 18669

International Patent Class: **H04L-009/00**
Fulltext Availability:
Detailed Description

Detailed Description
... trap host system is copied into the cage directory. As described more fully below, the **interface** to the operating system **kernel** is modified to **monitor** the **intruder** 's actions (e.g., by generating **log** data regarding an intruders activities), keep the intruder in the cage, and prevent the intruder...is copied to each of the cages, step 1704.
As has been described herein, the **interface** to the operating system **kernel** is modified to **monitor** the **intruder** 's actions, keep the **intruder** in the cage, and prevent the intruder from realizing

16/3,K/7   (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00922117   **Image available**

COMPUTER SECURITY AND MANAGEMENT SYSTEM

SYSTEME DE GESTION ET DE SECURITE INFORMATIQUE

Patent Applicant/Assignee:
  CISCO TECHNOLOGY INC, 170 West Tasman Road, San Jose, CA 95134, US, US (Residence), US (Nationality)

Inventor(s):
  ROWLAND Craig H, 6908 Dogwood Hollow, Austin, TX 78750, US,
  PETTIT Justin, 70 Redding Road, Campbell, CA 95008, US,
  RHODES Aaron, 642 West Maple Street, Clyde, OH 43410, US,
  IRWIN Vicki, 1703 Persimmon Road, Cedar Park, TX 78613, US,

Legal Representative:
  SHOWALTER Barton E (et al) (agent), Baker Botts L.L.P, 2001 Ross Avenue, Suite 600,, Dallas, TX 75201-2980, US,

Patent and Priority Information (Country, Number, Date):
  Patent: WO 200256152 A2-A3 20020718 (WO 0256152)
  Application: WO 2002US900 20020110 (PCT/WO US0200900)
  Priority Application: US 2001261155 20010110

Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
  AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
  EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
  LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI
  SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
  (EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
  (OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
  (AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
  (EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English
Filing Language: English
Fulltext Word Count: 14244

Main International Patent Class: **H04L-009/00**
International Patent Class: **H04L-009/32** ...

... **G06F-012/14**

Fulltext Availability:
  Detailed Description
  Claims

Detailed Description
... actions on the local system as requested by the MAC.
  The present invention has several **core** security and **intrusion** detection mechanisms such as **log** security in the form of **log** audit functions, login and logout anomaly detection fanctions; session monitors and a port scan detector...

Claim
... consisting of forensic evidence agent, intrusion control agent, file integrity agent, host scanning agent, known **intrusion** agent, loadable **kernel** module agent, password cracking agent, **log** archive agent, rootkit agent, suspicious file agent, promiscuous mode agent, hidden process detection agent, unauthorized...

16/3,K/14 (Item 14 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00772873 **Image available**
SYSTEM AND METHOD FOR GENERATING FICTITIOUS CONTENT FOR A COMPUTER
SYSTEME ET PROCEDE PERMETTANT DE GENERER UN CONTENU FICTIF POUR UN ORDINATEUR
Patent Applicant/Assignee:
RECOURSE TECHNOLOGIES INC, 2450 El Camino Real, #100, Palo Alto, CA 94306 , US, US (Residence), US (Nationality)
Inventor(s):
LYLE Michael, 2844 Buena Knoll Court, San Jose, CA 95121, US
ROSS Robert F, 151 Calderon #334, Mountain View, CA 94041, US
MARICONDO James R, 872 Ames Court, Palo Alto, CA 94303, US
Legal Representative:
JAMES William J, Ritter, Van Pelt & Yi LLP, Suite 205, 4906 El Camino Real, Los Altos, CA 94022, US
Patent and Priority Information (Country, Number, Date):

```
  Patent:               WO 200106373 A1 20010125 (WO 0106373)
  Application:          WO 2000US19222 20000714  (PCT/WO US0019222)
  Priority Application: US 99143821 19990714; US 99151531 19990830
```

Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

```
  AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB
  GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA
  MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA
  UG UZ VN YU ZA ZW
  (EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
  (OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
  (AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
  (EA) AM AZ BY KG KZ MD RU TJ TM
```

Publication Language: English
Filing Language: English
Fulltext Word Count: 12444

Main International Patent Class: **G06F-012/14**
Fulltext Availability:
Detailed Description

Detailed Description
... trap host system is copied into the cage directory. As described more fully below, the **interface** to the operating system **kernel** is modified to **monitor** the **intruder** 's actions (e.g., by generating **log** data regarding an intruders activities), keep the intruder in the cage, and prevent the
26...

```
Set     Items   Description
S1     295822   INTRUD? OR INTRUS? OR IDD OR IDDS OR IDS OR HONEY()POT? ? -
             OR SAND()BOX OR SANDBOX? OR NSM? OR THREAT()MONITOR? OR SURVE-
             IL? OR (ANOMAL? OR MISUSE?)(3N)(DETECT? OR MONITOR?)
S2     887154   KERNEL? OR CORE? OR CENTRAL()(PROGRAM? OR MODULE?) OR SYST-
             EM()(LEVEL? OR PROGRAM?)
S3     332467   BUFFER? OR CACHE? OR TEMPORAR?()(MEMOR? OR STORAGE?) OR CI-
             RCULAR()BUFFER?
S4      12073   DEVICE()DRIVER? OR DDL OR (PERIPHERAL? OR DEVICE)(N)(IO OR
             I()O OR INTERFACE?)
S5    2845173   AUDIT? OR MONITOR? OR LOG OR LOGS OR LOGGING OR LOGGED OR -
             HISTOR?
S6       6548   S1 AND S2
S7         62   S6 AND S3
S8          4   S6 AND S4
S9       1907   S6 AND S5
S10        20   S7 AND S5
S11        24   S8 OR S10
S12        19   RD (unique items)
S13        17   S12 NOT PY>2002
S14        16   S13 NOT PD>20011116
? show files
File   8:Ei Compendex(R) 1970-2005/Jan W3
         (c) 2005 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2005/Feb
         (c) 2005 ProQuest Info&Learning
File  65:Inside Conferences 1993-2005/Feb W4
         (c) 2005 BLDSC all rts. reserv.
File   2:INSPEC 1969-2005/Feb W3
         (c) 2005 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2005/Jan W3
         (c)2005 Japan Science and Tech Corp(JST)
File 111:TGG Natl.Newspaper Index(SM) 1979-2005/Feb 28
         (c) 2005 The Gale Group
File   6:NTIS 1964-2005/Feb W3
         (c) 2005 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2005/Feb W3
         (c) 2005 INIST/CNRS
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Feb W3
         (c) 2005 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-2005/Jan
         (c) 2005 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2005/Jan W3
         (c) 2005 FIZ TECHNIK
```

14/5/5 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

6461276 INSPEC Abstract Number: C2000-02-6130S-054

Title: A process state-transition analysis and its application to intrusion **detection**

Author(s): Nuansri, N.; Singh, S.; Dillon, T.S.
Author Affiliation: Dept. of Comput. Sci. & Comput. Eng., La Trobe Univ., Bundoora, Vic., Australia

Conference Title: Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99) p.378-87
Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA
Publication Date: 1999 Country of Publication: USA xvi+390 pp.
ISBN: 0 7695 0346 2 Material Identity Number: XX-1999-03025
U.S. Copyright Clearance Center Code: 0 7695 0346 2/99/$10.00
Conference Title: Proceedings of 15th Annual Computer Security Applications Conference
Conference Sponsor: Appl. Comput. Security Assoc.; ACM Special Interest Group on Security, Audit & Control
Conference Date: 6-10 Dec. 1999 Conference Location: Phoenix, AZ, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)

Abstract: This paper describes a new technique for detecting security breaches in a computer system. For each Unix process, the user credentials, which are user identifiers, determine the process privilege, including whether a process has gained a high privilege, such as that of the superuser. The state transition technique is applied to a suitably defined process state, identified by certain classes of user credential values. A transition takes place when these values change from one class to another. These states are clearly defined, and prohibited state transitions as well as some supporting rules are identified. When many break-ins succeed, either the rules are violated or these prohibited transitions occur, and this implies a violation of system security policy. A specially modified system call, ktrace0, is used by the superuser to **monitor** the process-state and state transition analysis is applied to the traced information, by the **Intrusion** Detection System. Tests show that most known security violations belonging to the targeted classes (such as **buffer** overflow exploits) can be detected (and possibly pre-empted) while the constituent activities are still being processed in the **kernel** . (21 Refs)

Subfile: C
Descriptors: security of data; Unix
Identifiers: process state transition analysis; security breach detection ; computer system; Unix process; user credential; user identifiers; process privilege; superuser; prohibited state transitions; break-ins; system call; ktrace; process state **monitoring** ; traced information; **Intrusion** Detection System
Class Codes: C6130S (Data security); C6150J (Operating systems)

14/5/7 (Item 1 from file: 6)
DIALOG(R)File 6:NTIS

2009818 NTIS Accession Number: AD-A324 562/8
Logging Kernel **Events**
Tera Computer Co., Seattle, WA.
Corp. Source Codes: 108307000; 420107
4 Dec 95 8p
Languages: English
Journal Announcement: GRAI9718

Product reproduced from digital image. Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)321-8547; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.

NTIS Prices: PC A02/MF A01
Country of Publication: United States

This document describes a feature to enhance the debugging facilities of the Tera operating system. In particular, it details a mechanism to **log kernel** events with minimal overhead and in a way that is non- **intrusive** to the developer or system administrator.

Descriptors: *Operating systems(Computers); *Debugging(Computers); Data management; Computer files; **Buffer** storage; Fields(Computer programs); Control sequences; C programming language

Identifiers: Tera operating system; C++ programming language; NTISDODXA

Section Headings: 62B (Computers, Control, and Information Theory--Computer Software)

14/5/9 (Item 2 from file: 144)
DIALOG(R)File 144:Pascal

15336377 PASCAL No.: 02-0023056

A useful intrusion **detection system prototype to** monitor **multi-processes based on system calls**

Information and communications security : Xian, 13-16 November 2001

HONGPEI LI; LIANLI CHANG; XINMEI WANG
SIHAN QING, ed; OKAMOTO Tatsuaki, ed; JIANYING ZHOU, ed
National Key Laboratory on Integrated Services Networks, Xidian University, Xi'an 710071, China

ICICS 2001 : international conference on information and communications security, 3 (Xian CHN) 2001-11-13
Journal: Lecture notes in computer science, 2001, 2229 441-450
ISBN: 3-540-42880-1 ISSN: 0302-9743 Availability: INIST-16343; 354000097031590480
No. of Refs.: 8 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: Germany; United States
Language: English

Based on studying of process behaviors classification, a practical **intrusion** detection system prototype is discussed. As one of the key elements, the system behaviors classifier (Naive Bayesian Classifier) can identify malicious system behaviors effectively by classifying the sequences of system calls as normal or abnormal. However, an extended **intrusion** detection mechanism by **monitoring** multiple processes to detect **intrusions** that can modify the behaviors of **system programs** (such as: Trojan Horses, **Buffer** overflow attacks, and viruses.) is proposed.

English Descriptors: Overflow(computer arithmetics); Bayes estimation; **Buffer** system; **Intrusion** detection systems; Prototype; Classification; **Monitoring** ; **Surveillance** ; Classifier; Bayes methods

French Descriptors: Depassement capacite; Estimation Bayes; Systeme tampon; Systeme detection **intrusion** ; Prototype; Classification; **Monitorage** ; **Surveillance** ; Classificateur; Methode Bayes

```
Set     Items   Description
S1         11   AU=(CROSBIE, M? OR CROSBIE M?)
S2          2   AU=(SHEPLEY R? OR SHEPLEY, R?)
S3        248   AU=(JONES, N? OR JONES N?)
S4          2   AU=(FRAYMAN, L? OR FRAYMAN L?)
S5          0   S1 AND S2 AND S3 AND S4
S6         14   (S1 OR S2 OR S3 OR S4) AND IC=G06F?
S7         14   IDPAT (sorted in duplicate/non-duplicate order)
S8         10   IDPAT (primary/non-duplicate records only)
File 347:JAPIO Nov 1976-2004/Oct(Updated 050208)
         (c) 2005 JPO & JAPIO
File 348:EUROPEAN PATENTS 1978-2005/Feb W03
         (c) 2005 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20050217,UT=20050210
         (c) 2005 WIPO/Univentio
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200513
         (c) 2005  Thomson Derwent
```

8/5/5 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014642295 **Image available**
WPI Acc No: 2002-462999/200249
Related WPI Acc No: 2002-443490
XRPX Acc No: N02-490547

Computer architecture for monitoring events occurring in computer system or network and analyzing events for signs of security violations has at least one correlation engine to interpret and analyze kernel audit and syslog data

Patent Assignee: CROSBIE M (CROS-I); FRAYMAN L L (FRAY-I); KUPERMAN B (KUPE-I); SHEPLEY R (SHEP-I)
Inventor: **CROSBIE M ; FRAYMAN L L** ; KUPERMAN B; **SHEPLEY R**
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020083343	A1	20020627	US 2000210922	A	20000612	200249	B
			US 2001878320	A	20010612		

Priority Applications (No Type Date): US 2000210922 P 20000612; US 2001878320 A 20010612
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020083343	A1		10	G06F-011/30	Provisional application US 2000210922

Abstract (Basic): US 20020083343 A

NOVELTY - A control agent (60) interfaces with a GUI system (55) and monitors system activity. At least one data gathering component gathers kernel audit data (70) and syslog data (72). At least one correlation engine (78) interprets and analyzes the kernel audit data and the syslog data using at least one detection template.

USE - As a host-based intrusion detection system (IDS) for monitoring events occurring in a computer system or network and analyzing the events for signs of security violations

ADVANTAGE - Observes kernel audit data, network packets and system log files on target host, provides more accurate determinations (fewer false positives, fewer missed attacks). Detects building blocks of attacks, not a variety of attack scenarios that may require frequent update. Detects insider attacks that do not use the network. Network traffic encryption has no impact.

DESCRIPTION OF DRAWING(S) - The drawing shows a high level illustration of the logical architecture according to the present invention.

GUI system 55
control agent 60
kernel audit data 70
syslog data 72
correlation engine 78
Dwg.1/5

Title Terms: COMPUTER; ARCHITECTURE; MONITOR; EVENT; OCCUR; COMPUTER; SYSTEM; NETWORK; EVENT; SIGN; SECURE; VIOLATION; ONE; CORRELATE; ENGINE; INTERPRETATION; ANALYSE; KERNEL; AUDIT; DATA
Derwent Class: T01
International Patent Class (Main): **G06F-011/30**
File Segment: EPI

```
 8/5/6     (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2005  Thomson Derwent. All rts. reserv.

014622786     **Image available**
WPI Acc No: 2002-443490/200247
Related WPI Acc No: 2002-462999
XRPX Acc No: N02-349423
  Intrusions detecting method in computer system, involves converting
  kernel records into ASCII format and comparing records against templates
  such as race conditions attack templates
Patent Assignee: CROSBIE M (CROS-I); FRAYMAN L L (FRAY-I); KUPERMAN B
  (KUPE-I); SHEPLEY R (SHEP-I)
Inventor:  CROSBIE M ;  FRAYMAN L L ; KUPERMAN B;  SHEPLEY R
Number of Countries: 001  Number of Patents: 001
Patent Family:
Patent No      Kind   Date    Applicat No    Kind   Date     Week
US 20020046275  A1  20020418  US 2000210922   P   20000612  200247  B
                              US 2001878319   A   20010612

Priority Applications (No Type Date): US 2000210922 P 20000612; US
  2001878319 A 20010612
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
US 20020046275 A1    29 G06F-015/16   Provisional application US 2000210922

Abstract (Basic): US 20020046275 A1
        NOVELTY - Kernel records containing a system call information and
    kernel audit logs converted into ASCII format and are compared against
    templates such as modification of files/directories templates, SetUID
    files templates, race conditions attack template. An alert message is
    generated based on the comparison result.
        DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the
    following:
        (1) Critical files/directories changes detecting method;
        (2) Method of detecting changes to log files; and
        (3) Method of detecting a race condition attack.
        USE - In host-based intrusion detection systems (IDSs) used in an
    enterprise environment for protecting host computer systems from
    exploits of known vulnerabilities, protecting from attacks coming in
    from network, for protecting against security policy violations within
    a system or enterprise and for protecting some applications and also
    for providing virus protection.
        ADVANTAGE - Detects intrusions accurately and communicates an alert
    and detailed information on the potential attack immediately.
        DESCRIPTION OF DRAWING(S) - The figure shows a high level
    illustration of the logical architecture.
        pp; 29 DwgNo 1/5
Title Terms: DETECT; METHOD; COMPUTER; SYSTEM; CONVERT; KERNEL; RECORD;
  ASCII; FORMAT; COMPARE; RECORD; TEMPLATE; RACE; CONDITION; ATTACK;
  TEMPLATE
Derwent Class: T01
International Patent Class (Main):  G06F-015/16
International Patent Class (Additional):  G06F-015/173
File Segment: EPI
```

```
Set     Items   Description
S1     641892   INTRUD? OR INTRUS? OR IDD OR IDDS OR IDS OR HONEY()POT? ? -
             OR SAND()BOX OR SANDBOX? OR NSM? OR THREAT()MONITOR? OR SURVE-
             IL? OR (ANOMAL? OR MISUSE?)(3N)(DETECT? OR MONITOR?)
S2    2742635   KERNEL? OR CORE? OR CENTRAL()(PROGRAM? OR MODULE?) OR SYST-
             EM()(LEVEL? OR PROGRAM?)
S3     469170   BUFFER? OR CACHE? OR TEMPORAR?()(MEMOR? OR STORAGE?) OR CI-
             RCULAR()BUFFER?
S4      90044   DEVICE()DRIVER? OR DDL OR (PERIPHERAL? OR DEVICE)(N)(IO OR
             I()O OR INTERFACE?)
S5    9716351   AUDIT? OR MONITOR? OR LOG OR LOGS OR LOGGING OR LOGGED OR -
             HISTOR?
S6       3931   S1 (10N) S2
S7          8   S6 (10N) S3
S8          0   S6 (10N) S4
S9        226   S6 (10N) S5
S10         2   S1(S)S2(S)S3(S)S4
S11       173   S1(S)S4
S12        33   S11(S)S5
S13        41   S12 OR S10 OR S7
S14        23   RD (unique items)
S15        15   S14 NOT PY>2001
S16        15   S15 NOT PD>20011116
File 275:Gale Group Computer DB(TM) 1983-2005/Mar 01
         (c) 2005 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2005/Feb 25
         (c) 2005 The Gale group
File  75:TGG Management Contents(R) 86-2005/Feb W3
         (c) 2005 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2005/Mar 01
         (c) 2005 The Gale Group
File  16:Gale Group PROMT(R) 1990-2005/Mar 01
         (c) 2005 The Gale Group
File 624:McGraw-Hill Publications 1985-2005/Mar 01
         (c) 2005 McGraw-Hill Co. Inc
File 484:Periodical Abs Plustext 1986-2005/Feb W3
         (c) 2005 ProQuest
File 613:PR Newswire 1999-2005/Mar 01
         (c) 2005 PR Newswire Association Inc
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 141:Readers Guide 1983-2004/Sep
         (c) 2004 The HW Wilson Co
File 239:Mathsci 1940-2005/Mar
         (c) 2005 American Mathematical Society
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS
File 696:DIALOG Telecom. Newsletters 1995-2005/Feb 28
         (c) 2005 The Dialog Corp.
File 553:Wilson Bus. Abs. FullText 1982-2004/Dec
         (c) 2005 The HW Wilson Co
File 621:Gale Group New Prod.Annou.(R) 1985-2005/Mar 01
         (c) 2005 The Gale Group
File 674:Computer News Fulltext 1989-2005/Feb W4
         (c) 2005 IDG Communications
File  88:Gale Group Business A.R.T.S. 1976-2005/Feb 28
         (c) 2005 The Gale Group
File 369:New Scientist 1994-2005/Feb W2
         (c) 2005 Reed Business Information Ltd.
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 635:Business Dateline(R) 1985-2005/Mar 01
         (c) 2005 ProQuest Info&Learning
File  15:ABI/Inform(R) 1971-2005/Mar 01
         (c) 2005 ProQuest Info&Learning
File   9:Business & Industry(R) Jul/1994-2005/Feb 28
         (c) 2005  The Gale Group
File  13:BAMP 2005/Feb W3
```

```
         (c) 2005  The Gale Group
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 610:Business Wire 1999-2005/Mar 01
         (c) 2005 Business Wire.
File 647:CMP  Computer Fulltext 1988-2005/Feb W2
         (c) 2005 CMP Media, LLC
File  98:General Sci Abs/Full-Text 1984-2004/Dec
         (c) 2005 The HW Wilson Co.
File 148:Gale Group Trade & Industry DB 1976-2005/Mar 01
         (c)2005 The Gale Group
File 634:San Jose Mercury  Jun 1985-2005/Feb 28
         (c) 2005 San Jose Mercury News
```

16/3,K/2 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2005 The Gale Group. All rts. reserv.

02318120 SUPPLIER NUMBER: 55276902 (USE FORMAT 7 OR 9 FOR FULL TEXT)
eSafe Protect Desktop 2.1.
PC Magazine, 18, 15, 107
Sept 1, 1999
ISSN: 0888-8507 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 488 LINE COUNT: 00042

... variety of actions upon discovering a virus and has a flexible scheduler as well.

The **sandbox** feature makes eSafe stand out in this roundup. eSafe uses Windows virtual **device drivers** to **monitor** operations by other programs, particularly Internet-enabled programs, and ensure that they don't misbehave...

16/3,K/10 (Item 1 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

095841
Get a positive ID on DDoS attackers
Mazu's TrafficMaster Inspector a good first step in identifying DDoS attacks.
Byline: MANDY ANDRESS
Journal: Network World Page Number: 55
Publication Date: August 27, 2001
Word Count: 1177 Line Count: 113

Text:
... on the network, but works best near the first-level routers, where it can directly **monitor** traffic to and from the Internet. Inspector connects to the data path via a passive...

...of network traffic from routers for analysis. Inspector sits directly on the network connection and **monitors** all traffic, independent of the network routers for packet information. One reason Mazu's solution...

... a great start in developing a fast, efficient distributed DoS solution. Its approach to separate **monitoring** and defense mechanisms does not make Inspector an optimal solution on its own. If we...
... three main components are at work: user-level Mazu module, Mazu Kernel module and Mazu **device driver** . The user-level module is the brains of the product. It performs the packet analysis...

... and routing to keep any latency introduced by its presence to an absolute minimum. The **device driver** optimizes packet processing, enabling Inspector to quickly and efficiently capture packets off the network. Initially...

... These administration tools provide four main functions: configuration, attack detection, attack characterization and traffic analysis **monitoring** .Configuration settings allow you to enable SNMP **monitoring** and set system thresholds. With SNMP enabled, an alert can be sent via your network ...

... overview page during the attack. The attack incident report page provides detailed information on attack **histories** and lets you drill down to specific packet details for each suspected attack.Inspector lets... identify distributed DoS attacks in large carrier-class networks. Starting at $100,000 for only **monitoring** and attack characterization, it is not a solution for the faint of heart. Overall, TrafficMaster Inspector provides fast, efficient **anomaly** -based **monitoring** , but it does not provide any filtering recommendations. To do that, administrators must create their...

```
Set     Items   Description
S1       1294   INTRUD? OR INTRUS? OR IDD OR IDDS OR IDS OR HONEY()POT? ? -
             OR SAND()BOX OR SANDBOX? OR NSM? OR THREAT()MONITOR? OR SURVE-
             IL? OR (ANOMAL? OR MISUSE?)(3N)(DETECT? OR MONITOR?)
S2       2291   KERNEL? OR CORE? OR CENTRAL()(PROGRAM? OR MODULE?) OR SYST-
             EM()(LEVEL? OR PROGRAM?)
S3        661   BUFFER? OR CACHE? OR TEMPORAR?()(MEMOR? OR STORAGE?) OR CI-
             RCULAR()BUFFER?
S4        114   DEVICE()DRIVER? OR DDL OR (PERIPHERAL? OR DEVICE)(N)(IO OR
             I()O OR INTERFACE?)
S5      10436   AUDIT? OR MONITOR? OR LOG OR LOGS OR LOGGING OR LOGGED OR -
             HISTOR?
S6         64   S1 AND S2
S7         11   S6 AND S3
S8          0   S6 AND S4
S9         46   S6 AND S5
S10         6   S1(5N)S2
S11         4   S9 AND S10
S12        13   S11 OR S7
S13         3   S12 NOT PD>20011116
File 256:TecInfoSource 82-2005/Jan
         (c) 2005 Info.Sources Inc
```

```
Set     Items   Description
S1      48217   INTRUD? OR INTRUS? OR IDD OR IDDS OR IDS OR HONEY()POT? ? -
             OR SAND()BOX OR SANDBOX? OR NSM? OR THREAT()MONITOR? OR SURVE-
             IL? OR (ANOMAL? OR MISUSE?)(3N)(DETECT? OR MONITOR?)
S2     506073   KERNEL? OR CORE? OR CENTRAL()(PROGRAM? OR MODULE?) OR SYST-
             EM()(LEVEL? OR PROGRAM?)
S3     281020   BUFFER? OR CACHE? OR TEMPORAR?()(MEMOR? OR STORAGE?) OR CI-
             RCULAR()BUFFER?
S4      12292   DEVICE()DRIVER? OR DDL OR (PERIPHERAL? OR DEVICE)(N)(IO OR
             I()O OR INTERFACE?)
S5     527815   AUDIT? OR MONITOR? OR LOG OR LOGS OR LOGGING OR LOGGED OR -
             HISTOR?
S6       1223   S1 AND S2
S7         15   S6 AND S3
S8          2   S6 AND S4
S9         93   S6 AND S5
S10         0   S9 AND IC=(G06F-017? OR G06F-007?)
S11        23   S9 AND IC=(G06F? OR H04L?)
S12        37   S7 OR S8 OR S11
S13        37   IDPAT (sorted in duplicate/non-duplicate order)
S14        37   IDPAT (primary/non-duplicate records only)
File 347:JAPIO Nov 1976-2004/Oct(Updated 050208)
         (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200513
         (c) 2005  Thomson Derwent
```

14/5/4 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

016698266 **Image available**
WPI Acc No: 2005-022542/200503
XRPX Acc No: N05-019466

Firewall framework for network device, has firewall engine with layer interface for returning action to requesting layer upon receiving layer parameters e.g. port number, for packet related to processor

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: MAYFIELD P G; SWANDER B D
Number of Countries: 038 Number of Patents: 006

```
Patent Family:
Patent No      Kind   Date     Applicat No     Kind   Date     Week
EP 1484884      A2  20041208  EP 20049147       A   20040416  200503  B
CA 2464784      A1  20041206  CA 2464784        A   20040419  200503
JP 2004362581   A   20041224  JP 2004165078     A   20040602  200503
ZA 200403075    A   20041229  ZA 20043075       A   20040422  200505
US 20050022010  A1   20050127  US 2003456766     A   20030606  200509
AU 2004202137   A1  20041223  AU 2004202137     A   20040519  200510

Priority Applications (No Type Date): US 2003456766 A 20030606
Patent Details:
Patent No  Kind Lan Pg   Main IPC     Filing Notes
EP 1484884    A2 E  31 H04L-029/06
   Designated States (Regional): AL AT BE BG CH CY CZ DE DK EE ES FI FR GB
   GR HR HU IE IT LI LT LU LV MC MK NL PL PT RO SE SI SK TR
CA 2464784    A1 E     H04L-009/00
JP 2004362581 A     43 G06F-013/00
ZA 200403075  A     57 G06F-000/00
US 20050022010 A1      H04L-009/00
AU 2004202137 A1       H04L-012/56
```

Abstract (Basic): EP 1484884 A2

NOVELTY - The framework has a set of layer processors, each processes layer parameters e.g. port number, for a packet related to the processor. Each processor issues a classification request with the parameters. A **kernel** firewall engine (256) has a layer interface to return an action to a requesting layer upon receiving the parameters. A lookup component identifies from a matching filter the action to be returned by the interface.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) a method of communicating between a layer process and a firewall process

(b) a computer-readable medium for executing computer-readable instructions for facilitating a firewall framework

(c) a computer-readable medium for executing computer-readable instructions for communicating between a layer process and a firewall process in an operating system.

USE - Used for providing multi-layering filtering of packet in a network device of a computer system that is utilized with personal computer, server computer, handheld or laptop device, multiprocessor system, microprocessor-based system, set top box, programmable consumer electronics, network PC, minicomputer and mainframe computer, distributed computing environment that includes above systems or devices.

ADVANTAGE - The firewall engine returns the action to the requesting layer upon receiving the parameters, thus permitting filtering of packets at all layers within a network stack, and hence providing more functionality such as **intrusion** detection, **logging** of packets and parental control features.

DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram illustrating firewall architecture.

Kernel firewall engine (256)
Filter engine application programmable interface (266)
Filters (282)

```
        Boot time policy (286)
        Filter module (294)
        pp; 31 DwgNo 3/9
Title Terms: FIREWALL; FRAMEWORK; NETWORK; DEVICE; FIREWALL; ENGINE; LAYER;
  INTERFACE; RETURN; ACTION; REQUEST; LAYER; RECEIVE; LAYER; PARAMETER;
  PORT; NUMBER; PACKET; RELATED; PROCESSOR
Derwent Class: T01; W01
International Patent Class (Main):  G06F-000/00 ;  G06F-013/00 ;
  H04L-009/00 ;  H04L-012/56 ;  H04L-029/06
International Patent Class (Additional):  G06F-001/00 ;  G06F-012/14 ;
  H04L-012/22 ;  H04L-012/66
File Segment: EPI
```

14/5/7. (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX

016269930 **Image available**
WPI Acc No: 2004-427824/200440

Kernel interface device **in** intrusion **detection system for system security and method therefor**

Patent Assignee: LGNSYS INC (LGNS-N)
Inventor: LEE H J
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2004015484	A	20040219	KR 200247750	A	20020813	200440	B

Priority Applications (No Type Date): KR 200247750 A 20020813
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2004015484	A		1	H04L-012/22	

Abstract (Basic): KR 2004015484 A

NOVELTY - A **kernel interface device** in an **IDS** (**Intrusion** Detection System) for system security and a method therefor are provided to **monitor** any event without exception by recognizing a **kernel** interface, which can execute **monitoring** and reporting for system event generation at the same with system booting, as a driver, software-type hardware, and making it operated in the early stage of booting.

DETAILED DESCRIPTION - A **kernel interface device** in an **IDS** (**Intrusion** Detection System) for system security consists of a ring '0' **monitor** driver(310), a ring '3' application program(330), and a **kernel** interface driver(320). The ring '0' **monitor** driver(310) **monitors** events of a ring '0' level for the transmission and reception of driver information between a ring '0' **kernel** mode and a ring '3' user mode. The ring '3' application program(330) is executed in the ring '3' user mode. The **kernel** interface driver(320) transmits the events **monitored** between the ring '0' **monitor** driver(310) and the ring '3' application program(330). The **kernel** interface driver(320) is comprised of a data channel(321), a cyclic data **buffer** (322), a system service thread(323), a **kernel** interface(331), and a synchronization information **buffer** (340).

pp; 1 DwgNo 1/10

Title Terms: **KERNEL** ; INTERFACE; DEVICE; **INTRUDE** ; DETECT; SYSTEM; SYSTEM ; SECURE; METHOD
Derwent Class: W01
International Patent Class (Main): **H04L-012/22**
File Segment: EPI

14/5/11 (Item 11 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015837343 **Image available**
WPI Acc No: 2003-899547/200382
XRPX Acc No: N03-717990

Profiling system for runtime environments, has profiling tool that creates runtime metric including application metric and non-application-code metric from software application and non-application-code component

Patent Assignee: AFGHANI A (AFGH-I); KARKARE A (KARK-I); MATHUS R (MATH-I); TSARIOUNOV A (TSAR-I)
Inventor: AFGHANI A; KARKARE A; MATHUS R; TSARIOUNOV A
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030192036	A1	20031009	US 2002120036	A	20020409	200382	B

Priority Applications (No Type Date): US 2002120036 A 20020409
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030192036	A1		25	G06F-009/45	

Abstract (Basic): US 20030192036 A1

NOVELTY - The system has a software application written in a platform-independent programming language. A non-application-code component is invoked by the software application. A profiling tool creates a runtime metric that includes an application metric and a non-application-code metric. The tool creates the application and non-application-code metrics from the software application and non-application-code component.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for a method of profiling the runtime environment of an application-code component.

USE - Used for runtime environments.

ADVANTAGE - The profiling tool can generate runtime profiles relating to both the software application and the non-application-code component invoked by the software application, thereby the system comprehensively profiles a runtime environment in a non- **intrusive** manner.

DESCRIPTION OF DRAWING(S) - The drawing shows a process-flow diagram of a **kernel** processing subsystem, and interactions between a **kernel** profiling subsystem and a virtual machine to generate comprehensive runtime metrics.

Profiler (45)
Virtual machine (62)
Kernel instrumentation trace (92)
Kernel instrumentation points (94)
Kernel instrumentation **buffer** (96)
Kernel instrumentation data (98)
pp; 25 DwgNo 10/12

Title Terms: PROFILE; SYSTEM; ENVIRONMENT; PROFILE; TOOL; METRIC; APPLY; METRIC; NON; APPLY; CODE; METRIC; SOFTWARE; APPLY; NON; APPLY; CODE; COMPONENT
Derwent Class: T01
International Patent Class (Main): G06F-009/45
File Segment: EPI

```
 14/5/15     (Item 15 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2005  Thomson Derwent. All rts. reserv.

014815395    **Image available**
WPI Acc No: 2002-636101/200268
XRPX Acc No: N02-502594
  Virus and  intrusion  protection apparatus for computer, has switch which
  when open disconnects main  core  of computer from dedicated network
  board, WWW and e-mail
Patent Assignee: LIN-HENDEL C (LINH-I)
Inventor: LIN-HENDEL C
Number of Countries: 001  Number of Patents: 001
Patent Family:
Patent No     Kind   Date    Applicat No    Kind   Date     Week
US 20020095607  A1  20020718  US 2001262966   A   20010118  200268  B
                             US 200252645    A   20020119

Priority Applications (No Type Date): US 2001262966 P 20010118; US
  200252645 A 20020119
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
US 20020095607 A1     9 G06F-012/14   Provisional application US 2001262966

Abstract (Basic): US 20020095607 A1
        NOVELTY - A dedicated network board (72) has duplicated computing
    components to isolate main  core  (74) of computer or network server
    from external communication with WWW (90). A switch (1A) when open
    disconnects the main  core  from the dedicated network board and WWW,
    e-mail and other external networks.
        DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for a
    method for protecting a computer from a virus, hacker or worm.
        USE - For protecting computer e.g. personal computer, laptop or
    computer networks from virus, hacker or worm.
        ADVANTAGE - Since the main  core  is never exposed to WWW and/or
    other external networks while communication sessions commence, no
    hacker, worm or virus can invade, infect or affect the main  core . The
     temporary  storage  media of the network board can be easily flushed
    and restored.
        DESCRIPTION OF DRAWING(S) - The figure shows a computer network
    with the virus and  intrusion  protection apparatus.
        Switch (1A)
        WWW (90)
        Dedicated network board (72)
        Main  core  of computer (74)
        pp; 9 DwgNo 2/2
Title Terms: VIRUS;  INTRUDE ; PROTECT; APPARATUS; COMPUTER; SWITCH; OPEN;
  DISCONNECT; MAIN;  CORE ; COMPUTER; DEDICATE; NETWORK; BOARD; MAIL
Derwent Class: T01
International Patent Class (Main): G06F-012/14
File Segment: EPI
```

```
 14/5/17     (Item 17 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2005  Thomson Derwent. All rts. reserv.

014642295     **Image available**
WPI Acc No: 2002-462999/200249
Related WPI Acc No: 2002-443490
XRPX Acc No: N02-490547
  Computer architecture for  monitoring  events occurring in computer
  system or network and analyzing events for signs of security violations
  has at least one correlation engine to interpret and analyze  kernel
  audit  and syslog data
Patent Assignee: CROSBIE M (CROS-I); FRAYMAN L L (FRAY-I); KUPERMAN B
  (KUPE-I); SHEPLEY R (SHEP-I)
Inventor: CROSBIE M; FRAYMAN L L; KUPERMAN B; SHEPLEY R
Number of Countries: 001  Number of Patents: 001
Patent Family:
Patent No     Kind   Date    Applicat No    Kind   Date     Week
US 20020083343  A1  20020627  US 2000210922   A   20000612  200249  B
                             US 2001878320   A   20010612

Priority Applications (No Type Date): US 2000210922 P 20000612; US
  2001878320 A 20010612
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
US 20020083343 A1    10 G06F-011/30   Provisional application US 2000210922

Abstract (Basic): US 20020083343 A
        NOVELTY - A control agent (60) interfaces with a GUI system (55)
    and  monitors  system activity. At least one data gathering component
    gathers  kernel   audit  data (70) and syslog data (72). At least one
    correlation engine (78) interprets and analyzes the  kernel   audit
    data and the syslog data using at least one detection template.
        USE - As a host-based  intrusion  detection system (  IDS  ) for
     monitoring  events occurring in a computer system or network and
    analyzing the events for signs of security violations
        ADVANTAGE - Observes  kernel   audit  data, network packets and
    system  log  files on target host, provides more accurate
    determinations (fewer false positives, fewer missed attacks). Detects
    building blocks of attacks, not a variety of attack scenarios that may
    require frequent update. Detects insider attacks that do not use the
    network. Network traffic encryption has no impact.
        DESCRIPTION OF DRAWING(S) - The drawing shows a high level
    illustration of the logical architecture according to the present
    invention.
        GUI system 55
        control agent 60
         kernel   audit  data 70
        syslog data 72
        correlation engine 78
        Dwg.1/5
Title Terms: COMPUTER; ARCHITECTURE;  MONITOR ; EVENT; OCCUR; COMPUTER;
  SYSTEM; NETWORK; EVENT; SIGN; SECURE; VIOLATION; ONE; CORRELATE; ENGINE;
  INTERPRETATION; ANALYSE;  KERNEL ;  AUDIT ; DATA
Derwent Class: T01
International Patent Class (Main):  G06F-011/30
File Segment: EPI
```

```
 14/5/25     (Item 25 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2005  Thomson Derwent. All rts. reserv.

012470797     **Image available**
WPI Acc No: 1999-276905/199923
XRPX Acc No: N99-207620
  System performance  monitoring  method for single processor and
  multiprocessor system - involves displaying call count and data collected
  after execution of instrumentation phase for each selected code segment
  which are selected during burst counting phase
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC  )
Inventor: BLANDY G O; SABA M A; URQUHART R J
Number of Countries: 001  Number of Patents: 001
Patent Family:
Patent No     Kind   Date    Applicat No    Kind   Date     Week
US 5896538     A   19990420  US 96753570     A   19961126  199923  B

Priority Applications (No Type Date): US 96753570 A 19961126
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
US 5896538    A     18 G06F-009/45

Abstract (Basic): US 5896538 A
        NOVELTY - A burst counting phase is executed and then execution is
    switched over to an instrumentation phase, when predetermined number of
    code segments are selected in burst counting phase. Instrumentation
    phase for each selected code segment is executed and call count and
    data collected for each segment during execution is displayed in a
    display device. DETAILED DESCRIPTION - During burst counting phase,
    predetermined number of instructions are executed and call count for
    one or more code segments is stored. The call count indicates number of
    times a particular code segment is executed. Then one or more code
    segments are selected and call count for each segment is equal to a
    predetermined value. After display of call count and data, switching
    over to burst counting phase from instrumentation phase is performed,
    when selected code segment completes execution.
        USE - For single processor and multiprocessor system.
        ADVANTAGE - Enables programmer to improve performance of system as
    statistic summary of system is presented to user after dividing into
    user code and  kernel  code. Identifies frequently executed code paths
    in system with minimum  intrusion  to system function and minimum usage
    of memory capacity. DESCRIPTION OF DRAWING(S) - The figure shows block
    diagram illustrating system performance  monitoring  method.
        Dwg.2/11
Title Terms: SYSTEM; PERFORMANCE;  MONITOR ; METHOD; SINGLE; PROCESSOR;
  MULTIPROCESSOR; SYSTEM; DISPLAY; CALL; COUNT; DATA; COLLECT; AFTER;
  EXECUTE; INSTRUMENT; PHASE; SELECT; CODE; SEGMENT; SELECT; BURST; COUNT;
  PHASE
Derwent Class: T01
International Patent Class (Main):  G06F-009/45
File Segment: EPI
```

```
 14/5/27     (Item 27 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2005  Thomson Derwent. All rts. reserv.

010472905    **Image available**
WPI Acc No: 1995-374225/199549
XRPX Acc No: N95-276023
   Intrusion  and  misuse   detection  system for data processing system -
  has misuse engine which compares states of system inputs to predetermined
  states, and output mechanism produces notification signal upon  detection
   of  misuse
Patent Assignee: SMAHA S E (SMAH-I); NETWORKS ASSOC INC (NETW-N); HAYSTACK
  LABS INC (HAYS-N)
Inventor: SMAHA S E; SNAPP S R
Number of Countries: 002  Number of Patents: 003
Patent Family:
Patent No     Kind   Date     Applicat No    Kind   Date     Week
CA 2144105     A   19950908  CA 2144105      A   19950307  199549  B
US 5557742     A   19960917  US 94208019     A   19940307  199643
CA 2144105     C   19990817  CA 2144105      A   19950307  199953

Priority Applications (No Type Date): US 94208019 A 19940307
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
CA 2144105    A     73 G06F-012/14
US 5557742    A     46 G06F-011/34
CA 2144105    C  E     G06F-012/14

Abstract (Basic): CA 2144105 A
        The intrusion  and  misuse  detection  system (10) for data
    processing system uses processing system inputs. This includes
    processing system  audit  trail records (18), system  log  file data
    (16), and system security state data (14). A misuse selector (20)
    allows the detection system to analyse the process inputs for a
    selected subset of misuses.
        The processing system inputs are then converted into states which
    are compared, through a misuse engine (30), to a predefined set of
    states and transitions until a selected  misuse  is  detected . Once a
    misuse  has been  detected , an output mechanism generates a signal for
    use by notification and storage mechanism. The detection system then
    generates a text-based output report for a user to view or store.
        ADVANTAGE - Minimises number of false positives. Eliminates need
    for expert programming. Improved efficiency and simplified development
    and testing.
        Dwg.1/6
Title Terms:  INTRUDE ; MISUSE; DETECT; SYSTEM; DATA; PROCESS; SYSTEM;
  MISUSE; ENGINE; COMPARE; STATE; SYSTEM; INPUT; PREDETERMINED; STATE;
  OUTPUT; MECHANISM; PRODUCE; NOTIFICATION; SIGNAL; DETECT; MISUSE
Derwent Class: T01
International Patent Class (Main):  G06F-011/34 ;  G06F-012/14
File Segment: EPI
```

14/5/32 (Item 32 from file: 347)
DIALOG(R)File 347:JAPIO

06786758 **Image available**
SECURITY SYSTEM BY MULTIPLEX SYSTEM PARALLEL OPERATED COMPUTERS

PUB. NO.: 2001-014239 [JP 2001014239 A]
PUBLISHED: January 19, 2001 (20010119)
INVENTOR(s): FURUKAWA HIROSHI
SHINOHARA DAISUKE
OSHIMA SATOSHI
UCHIYAMA YASUFUMI
APPLICANT(s): HITACHI LTD
APPL. NO.: 11-182908 [JP 99182908]
FILED: June 29, 1999 (19990629)
INTL CLASS: **G06F-013/00** ; **G06F-012/14** ; **G06F-015/00**

ABSTRACT

PROBLEM TO BE SOLVED: To secure the security of systems to be simultaneously and parallel operated without altering the systems by making a **monitoring** system **monitor** the contents of inter-system communications with the other system and an illegal inter-system communication control from the other system and preventing the influence of an illegal **intrusion** and control when an illegality is detected except for the **monitoring** system.

SOLUTION: A multiplex system parallel operation **kernel** 300 simultaneously and parallel operates plural systems on one computer. A system interruption control part 301 controls the interruption between respective systems and performs assigning or scheduling of processors. Besides, a system operation memory space managing part 302 manages the memories of respective systems and assigns memories for each of respective systems. When an illegal access is performed from one system to the multiplex system parallel operation **kernels** 300, the multiplex system parallel operation **kernel** 300 enables a general system itself to stop while using a system start/end control part 304.